Discrete Mathematics 94 (1991) 229–232
North-Holland

Note

All binary codes with covering radius one are subnormal

Iiro Honkala

Department of Mathematics, University of Turku, 20500 Turku 50, Finland

Received 4 May 1989
Revised 7 March 1990

Abstract

Honkala, I., All binary codes with covering radius one are subnormal, Discrete Mathematics 94 (1991) 229–232.

We prove that if a binary code has covering radius one then it is subnormal.

1. Introduction

Covering radius problems are currently of great interest in coding theory. Suppose $C \subseteq \mathbb{F}_2^n$ is a binary code, a non-empty set of binary words of length n. By definition, the covering radius of the code C is the smallest integer R with the following property: given any binary word $x \in \mathbb{F}_2^n$, we can find a codeword $c \in C$ such that x and c disagree in at most R coordinates. If a binary code $C \subseteq \mathbb{F}_2^n$ has covering radius R and there are M codewords in C, we say that C is an $(n, M)R$ code. We define

$$K(n, R) = \min\{M \mid \text{there is an } (n, M)R \text{ code}\}.$$

Many results about this function can be found in [1–2, 5, 9] and their references. Any $(n, M)R$ code with $M = K(n, R)$ is called *optimal*. If $x, y \in \mathbb{F}_2^n$, we denote by $d(x, y)$ their Hamming distance, the number of coordinates in which they differ from each other, and denote $d(x, S) = \min_{s \in S} d(x, s)$. We say that an $(n, M)R$ code C is *subnormal* if there is a subset C_1 of C such that

$$d(x, C_1) + d(x, C \setminus C_1) \leq 2R + 1 \quad \text{for all } x \in \mathbb{F}_2^n.$$

(We define $d(x, \emptyset) = n$.) If, furthermore, we can choose

$$C_1 = C_0^{(i)} = \{c \in C \mid c(i) = 0\}$$

for some i, then C is called *normal* (here $c(i)$ denotes the ith coordinate of c). Otherwise, we call C *absubnormal* and *abnormal*, respectively. It is possible to combine efficiently two normal codes (or a normal and a subnormal code) using the amalgamated direct sum construction, see [2, 5]. These two concepts are also related to the conjecture [2] that

$$K(n+2, R+1) \leq K(n, R), \qquad n \neq R. \tag{1}$$

If we were able to show that all binary codes are subnormal then (1) would follow; see [4]. In fact, it would even be sufficient to show that for every n and R there is an $(n, K(n, R))R$ code C for which we can find a subset C_1 satisfying $d(x, C_1) + d(x, C \setminus C_1) \leq 2R+1$ for all $x \in \mathbb{F}_2^n$ such that $d(x, C) = R$. In this note we consider binary codes with covering radius one. All binary linear codes with covering radius one and all optimal binary codes with covering radius one are known to be normal; see [2, 6, 10]. Consequently, (1) holds for $R = 1$ (see also [5] and its references). It is also known that there are abnormal binary codes with covering radius one; see [7, 6]. In this note, however, we show that all binary codes with covering radius one are subnormal. No absubnormal binary codes are currently known.

2. The result

We now assume that C is an $(n, M)1$ code. If

$$d(x, C_0^{(i)}) + d(x, C_1^{(i)}) > 3$$

then following [2] we say that x is bad for i. We denote $e_j = 0^{j-1}10^{n-j}$. The proof of our result is based on the following lemma [6, Lemma 1].

Lemma. *If C is an $(n, M)1$ code and $x \in \mathbb{F}_2^n$ is bad for i, then $x \in C$ or $x + e_i \in C$. If $x \in C$ is bad for i then $x + e_j \in C$ for all $j \neq i$.*

Theorem. *If C is an $(n, M)1$ code then C is subnormal.*

Proof. Consider some fixed coordinate i, and denote $A = \{x \in C \mid x \text{ is bad for } i\}$. If $A = \emptyset$ then C is even normal, so we assume that $A \neq \emptyset$. Let T be a maximal subcode of A which has minimum distance two, i.e., $d(c_1, c_2) \geq 2$ for all $c_1, c_2 \in T$, and $d(c, T) \leq 1$ for all $c \in A \setminus T$. For every $t \in T$ we have, by the Lemma,

$$F_t = \{t\} \cup \{t + e_j \mid j \neq i\} \subseteq C$$

and $F_t \subseteq C_0^{(i)}$ or $F_t \subseteq C_1^{(i)}$. We choose

$$C_1 = (C_0^{(i)} \cup T_1^{(i)}) \setminus T_0^{(i)}, \qquad C_2 = (C_1^{(i)} \cup T_0^{(i)}) \setminus T_1^{(i)}.$$

Then clearly $C_1 \cup C_2 = C$, and we claim that for this choice

$$d(x, C_1) + d(x, C_2) \leq 3 \quad \text{for all } x \in \mathbb{F}_2^n.$$

This will prove the result.

Suppose first that $d(x, t) \leq 2$ for some $t \in T$. Assume further that $t \in C_0^{(i)}$ (the case $t \in C_1^{(i)}$ is similar). Then by the Lemma and the definitions of C_1 and C_2.

$$t \in C_2, \qquad t + e_j \in C_1 \quad \text{for all } j \neq i.$$

If $d(x, t) = 2$, then $d(x, C_1) \leq 1$ and $d(x, C_2) \leq 2$; if $d(x, t) = 1$, then $d(x, C_1) \leq 2$ and $d(x, C_2) \leq 1$; if $d(x, t) = 0$, then $d(x, C_1) \leq 1$ and $d(x, C_2) = 0$. Anyway, $d(x, C_1) + d(x, C_2) \leq 3$.

We can therefore assume that $d(x, T) \geq 3$ (and $n \geq 3$). If x were bad for i then by the Lemma $x \in A$ or $x + e_i \in A$, but $d(x, T) \geq 3$ and $d(x + e_i, T) \geq 2$ would contradict the maximality of T. Thus x is not bad for i, i.e., there are codewords $c_0 \in C_0^{(i)}$ and $c_1 \in C_1^{(i)}$ such that $d(x, c_0) + d(x, c_1) \leq 3$ (or $n = 3$, $C_0^{(i)} = \emptyset$, $x \in C_1^{(i)}$ (or vice versa) in which case $d(x, C_1) + d(x, C_2) \leq 3$ clearly holds). If $c_0 \notin T$ and $c_1 \notin T$ then we are already done. Clearly $c_0 \in T$, $c_1 \in T$ is not possible because $d(x, T) \geq 3$. Assume therefore that $c_0 \in T$, $c_1 \notin T$ (the case $c_0 \notin T$, $c_1 \in T$ is similar). Because $d(x, c_0) + d(x, c_1) \leq 3$ and $d(x, T) \geq 3$ we have $d(x, c_0) = 3$, $x = c_1$. Now $c_0 \in C_2$, $c_1 \in C_2$, and it is sufficient to find a codeword $c \in C_1$ such that $d(x, c) \leq 3$. By the Lemma $c_0 + e_j \in C$ for all $j \neq i$. Choose now j in such a way that $d(x, c_0 + e_j) = 2$. Then $c_0 + e_j \in C_0^{(i)}$ and $c_0 + e_j \notin T$ since T has minimum distance two, and consequently $c_0 + e_j \in C_1$.

This completes the proof of the Theorem. □

Acknowledgment

The author would like to thank Heikki Hämäläinen and the referees for useful remarks.

References

[1] G.D. Cohen, M.R. Karpovsky, H.F. Mattson Jr and J.R. Schatz, Covering radius—survey and recent results, IEEE Trans. Inform. Theory 31 (1985) 328–343.

[2] G.D. Cohen, A.C. Lobstein and N.J.A. Sloane, Further results on the covering radius of codes, IEEE Trans. Inform. Theory 32 (1986) 680–694.

[3] R.L. Graham and N.J.A. Sloane, On the covering radius of codes, IEEE Trans. Inform. Theory 31 (1985) 385–401.

[4] I.S. Honkala, Lower bounds for binary covering codes, IEEE Trans. Inform. Theory 34 (1988) 326–329.

[5] I.S. Honkala, Modified bounds for covering codes, IEEE Trans. Inform. Theory 37 (1991) 351–365.

[6] I.S. Honkala and H.O. Hämäläinen, Bounds for abnormal binary codes with covering radius one, IEEE Trans. Inform. Theory 37 (1991) 372–375.

[7] K.E. Kilby and N.J.A. Sloane, On the covering radius problem for codes II. Codes of low dimension; normal and abnormal codes, SIAM J. Algebraic Discrete Methods 8 (1987) 619–627.
[8] A.C. Lobstein and G.J.M. van Wee, On normal and subnormal q-ary codes, IEEE Trans. Inform. Theory 35 (1989) 1291–1295 and 36 (1990) 1498.
[9] G.J.M. van Wee, Improved sphere bounds on the covering radius of codes, IEEE Trans. Inform. Theory 34 (1988) 237–245.
[10] G.J.M. van Wee, More binary covering codes are normal, IEEE Trans. Inform. Theory 36 (1990) 1466–1470.